intel®

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR PATENT

ON

RADIO FREQUENCY IDENTIFICATION TAG LOCK AND KEY

INVENTOR:

Mark D. Yarvis

PREPARED AND SUBMITTED BY:

Kenneth J. Cool
Senior Patent Attorney
Intel Corporation
Tel. (408) 850-1229
Fax (408) 716-2586

Express Mail Label No.: **EL 962029193 US**

Docket No. P18388

RADIO FREQUENCY IDENTIFICATION TAG LOCK AND KEY

BACKGROUND OF THE INVENTION

[0001] The present invention relates generally to the field of radio frequency identification (RFID) tags. RFID tags are typically utilized to detect the presence or identity of a physical object wherein an RFID tag attached to the object may be detected, although the scope of the invention is not limited in this respect.

DESCRIPTION OF THE DRAWING FIGURES

[0002] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features, and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanying drawings in which:

[0003] FIG. 1 is a block diagram of a lock and key programming architecture to program a pair of radio frequency identification tags in accordance with one embodiment of the present invention;

[0004] FIG. 2 is a block diagram of a lock and key detection architecture to detect an RIFD lock tag and key tag pair in accordance with one embodiment of the present invention;

[0005] FIG. 3 is a data flow diagram of a method to detect a lock and key using a public cryptography key in accordance with one embodiment of the present invention;

[0006] FIG. 4 is a block diagram of a lock and key detection architecture using symmetric key cryptography in accordance with an embodiment of the present invention; and

[0007] FIG. 5 is a data flow diagram of a method to detect a lock and key using a symmetric cryptography key in accordance with an embodiment of the present invention.

[0008] It will be appreciated that for simplicity and clarity of illustration, elements illustrated in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements are exaggerated relative to other elements for clarity. Further, where considered appropriate, reference numerals have been repeated among the figures to indicate corresponding or analogous elements.

DETAILED DESCRIPTION

[0009] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the present invention.

[0010] Some portions of the detailed description that follows are presented in terms of algorithms and symbolic representations of operations on data bits or binary digital signals within a computer memory. These algorithmic descriptions and representations may be the

techniques used by those skilled in the data processing arts to convey the substance of their work to others skilled in the art.

[0011] An algorithm is here, and generally, considered to be a self-consistent sequence of acts or operations leading to a desired result. These include physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be understood, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

[0012] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as processing, computing, calculating, determining, or the like, refer to the action or processes of a computer or computing system, or similar electronic computing device, that manipulate or transform data represented as physical, such as electronic, quantities within the registers or memories of the computing system into other data similarly represented as physical quantities within the memories, registers or other such information storage, transmission or display devices of the computing system.

[0013] Embodiments of the present invention may include apparatuses for performing the operations herein. This apparatus may be specially constructed for the desired purposes, or it may comprise a general purpose computing device selectively activated or reconfigured by a program stored in the device. Such a program may be stored on a storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), electrically programmable read-only memories (EPROMs), electrically erasable and programmable read

only memories (EEPROMs), flash memory, magnetic or optical cards, or any other type of media suitable for storing electronic instructions, and capable of being coupled to a system bus for a computing device.

[0014] The processes and displays presented herein are not inherently related to any particular computing device or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct a more specialized apparatus to perform the desired method. The desired structure for a variety of these systems will appear from the description below. In addition, embodiments of the present invention are not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

[0015] In the following description and claims, the terms coupled and connected, along with their derivatives, may be used. In particular embodiments, connected may be used to indicate that two or more elements are in direct physical or electrical contact with each other. Coupled may mean that two or more elements are in direct physical or electrical contact. However, coupled may also mean that two or more elements may not be in direct contact with each other, but yet may still cooperate or interact with each other.

[0016] It should be understood that embodiments of the present invention may be used in a variety of applications. Although the present invention is not limited in this respect, the circuits disclosed herein may be used in many apparatuses such as in the transmitters and receivers of a radio system. Radio systems intended to be included within the scope of the present invention include, by way of example only, wireless local area networks (WLAN) devices and wireless wide area network (WWAN) devices including wireless network interface devices and network interface cards (NICs), base stations, access points (APs), gateways, bridges, hubs, cellular radiotelephone communication systems, satellite communication systems,

two-way radio communication systems, one-way pagers, two-way pagers, personal communication systems (PCS), personal computers (PCs), personal digital assistants (PDAs), and the like, although the scope of the invention is not limited in this respect.

[0017] Types of wireless communication systems intended to be within the scope of the present invention include, although not limited to, Wireless Local Area Network (WLAN), Wireless Wide Area Network (WWAN), Code Division Multiple Access (CDMA) cellular radiotelephone communication systems, Global System for Mobile Communications (GSM) cellular radiotelephone systems, North American Digital Cellular (NADC) cellular radiotelephone systems, Time Division Multiple Access (TDMA) systems, Extended-TDMA (E-TDMA) cellular radiotelephone systems, third generation (3G) systems like Wide-band CDMA (WCDMA), CDMA-2000, and the like, although the scope of the invention is not limited in this respect.

[0018] Referring now to FIG. 1, a block diagram of a lock and key programming architecture to program a pair of radio frequency identification (RFID) tags in accordance with the present invention will be discussed. As shown the programming architecture 100 of FIG. 1, during a programming phase a programming module 110 may create a matching pair of tags, a lock tag 112 and key tag 114, using one or more RFID readers, RFID reader 116 and RFID reader 118. In one embodiment of the invention, RFID reader 116 may be the same device as RFID reader 118, and in an alternative embodiment RFID reader 116 may be a device separate from RFID reader 118, and furthermore RFID reader 116 may be separated from RFID reader 118 in space or time, although the scope of the invention is not limited in this respect. It is not required that lock tag 112 and key tag 114 be created at the same time or at the same location. In one embodiment of the invention, when lock tag 112 and key tag 114 are not created at the same time or at the same location, programming module 110 may store information to create the other tag of the matching pair of RFID tags at a later time. Furthermore, in one particular embodiment of the invention, programming module 110 may create more than one identical lock tag 112 or

more than one identical key tag 114 wherein the key tags 114 may match the lock tags 112 in the set, although the scope of the invention is not limited in this respect.

[0019] One application of lock and key programming architecture 100 may be for amusement park security or the like. In such an application, for example, one lock tag 112 may be created for a child and one key tag 114 may be created for each parent or guardian of the child. Detection of a lock tag 112 and a key tag 114 may occur at the park gates, for example using a lock and key detection architecture 200 as shown in and described with respect to FIG. 2. If a child having a lock tag 112 were to attempt leave the park without a parent or guardian present having a corresponding key tag 114, an alarm may sound and the child may be prevented from leaving the park. In another example application of lock and key programming architecture, 100 such as in a department store for example, a lock tag 112 may be affixed to a product, and the lock tag 112 may be additionally tamper-resistant, when the product is stock on a shelf. Detection of a lock tag 112 and a key tag 114 may occur at the front door of the store, fore example using the lock and key detection architecture 200 of FIG. 2. A key tag 114 corresponding to the lock tag 112 of the product may be generated by the register at checkout and affixed to the receipt of payment. During detection at the front door of the store, if an attempt was made to exit the store with the product but without the corresponding appropriate receipt having the key tag 114, an alarm may sound. In at least one embodiment of the invention, information stored on one or both of lock tag 112 and key tag 114 may be a secret, may be encoded, and the tags may further be tamper resistant, although the scope of the invention is not limited in this respect.

[0020] Referring now to FIG. 2, a lock and key detection architecture to detect an RIFD lock tag and key tag pair in accordance with one embodiment of the invention will be discussed. As shown in FIG. 2, the lock and key detection architecture 200 may be controlled by a detection module 210 that may be connected to an RFID reader 212. In one embodiment of the invention, RFID reader 212 may be the same device as a either one or both of RFID reader 116 and 118, or may be a separate RFID reader disposed at a location separate from the location of either one or

both of RFID reader 116 and RFID reader 118. In one embodiment of the invention, lock and key detection architecture 200 may identify one or more lock tags 112 that may be present, for example within an operational range of RFID reader, and may detect the presence or absence of one or more matching key tags 114 that are also present, for example within an operational range of RFID reader 212, optionally within a predetermined time window, for the one or more present lock tags 112, although the scope of the invention is not limited in this respect.

[0021] In one embodiment of the invention, the detection of the presence of a lock tag 112, or the announcement of the presence of a lock tag 112, may be considered as trusted since in the event of a spoof or an attack, a false alarm may be generated and dealt with accordingly. Typically, either one or both of lock tag 112 or key tag 114 may not trusted to perform verification since in the event of a spoof or an attack, a false verification may occur, although the scope of the invention is not limited in this respect. In accordance with one embodiment of the present invention, a challenge and response architecture such as the key detection architecture 200 may be utilized to validate that a key tag 114 matches a given lock tag 112, although the scope of the invention is not limited in this respect.

[0022] In one embodiment of the invention, public key cryptography may be utilized to ensure proper validation of key tag 114. In such an embodiment, during a programming phase as implemented by lock and key programming architecture 100, lock tag 112 may be given a public key, and key tag 114 may be given a matching private key. In the event both lock tag 112 and key tag 114 are not created at the same time, for example as in the a department store example, then a private key that matches the public key may be securely stored to allow subsequent programming of key tag 114.

[0023] As shown in FIG. 2, a challenge and response protocol may be implemented by lock and key detection architecture 200. RFID reader 212 may initiate detection by periodically sending an activation signal to RFID tags that may be in the vicinity that is within the operating

range of RFID reader 212. In the event one or more lock tags 112 are present, the lock tags 112 respond to RFID reader 212 with their public keys. Such public key information may not be a secret, and RFID tag 212 may be delivered to detection module 210 for use in preparation of a challenge for one or more of the lock tags 112. The challenges may be utilized to identify one or more paired key tags 114. Detection module 210 sends a challenge as part of a subsequent activation signal from the RFID reader. If one or more corresponding key tags 114 are present, the one or more key tags 114 may utilize their private keys to formulate and send an appropriate challenge response. If an appropriate challenge response is not received within a predetermined timeout period, detection module 210 may signal an alarm.

[0024] Referring now to FIG. 3, a data flow diagram of a method to detect a lock and key using a public cryptography key in accordance with an embodiment of the invention will be discussed. As shown in the method 300 of FIG. 3, detection module 210 may generate a challenge by generating a random nonce at block 310 and encrypting the random nonce at block 312 using the public key obtained from lock tag 112 at block 314. In at least one embodiment of invention, a nonce may be defined as a random value or string utilized in authentication protocols, although the scope of the invention is not limited in this respect. The challenge may then sent to one or more key tags 114 present in the vicinity of detection module 210, and the nonce otherwise may be kept secret. When key tag 114 receives the challenge, key tag 114 may utilize its private key at block 316 to decrypt the nonce at block 318. Key tag 114 may then send the decrypted nonce back to detection module 210 for verification. The nonce may not be protected during a challenge response, as the nonce no longer may be a secret in the presence of an authorized key tag 114. Once detection module 210 receives a correct nonce, as determined by comparing at comparing block 320 the nonce received from key tag 114 to the nonce generated at block 310, a valid key tag is determined to be present, and no alarm is sounded. In the event it is determined at the comparing block 320 that the nonce generated at block 310 does not match the nonce sent to detection module 210 by key tag 114, and optionally within a predetermined time window or timeout period, a valid key tag 114 is not determined to be present, and alarm block 322 may generate an alarm, although the scope of the invention is not limited in this respect.

[0025] Referring now to FIG. 4, a lock and key detection architecture using symmetric key cryptography in accordance with an embodiment of the present invention will be discussed. To allow validation of a key tag 114 by utilizing symmetric key cryptography, the same key may be placed on both lock tag 112 and key tag 114 during a programming phase such as a programming phase implemented by lock and key programming architecture 100. During a detection phase, a key tag 114 may prove that it holds the same key as a lock tag 112 without requiring disclosure of the key. As with a challenge and response using a public cryptography key as shown in FIG. 3, detection of a symmetric cryptography using detection module 210 may also implement a challenge and response protocol. As shown in FIG. 4, detection module 210 may generate and send a randomly generated nonce at a regular interval, thereby forming a stream of nonces. The RFID tags may receive the nonces broadcast from detection module 210 and may utilize their own keys to encrypt the nonces and to generate a response, thereby forming a response stream. In one embodiment of the invention, the response stream broadcast by one or more lock tags 112 may be delayed by one cycle, for example the responses from lock tags 112 may be an encryption of a previous nonce, although the scope of the invention is not limited in this respect.

[0026] Referring now to FIG. 5, a data flow diagram of a method to detect a lock and key using a symmetric cryptography key in accordance with the present invention will be discussed. As shown in the method 500 of FIG. 5, to determine the validity of a key tag 114, detection module 210 may send generate a nonce at block 510. Key tag 114 may utilize its key at block 512 to encrypt a response at block 514 that is sent to detection module 210. Detection module 210 may receive the encrypted response from key tag 114, wait one cycle at queue block 516, and then send a subsequent nonce generated at block 510. Lock tag 112 may receive the nonce originally generated by detection module 210 at block 510, wait one cycle at queue block 518, and then utilize the key at key block 520 to encrypt the key at block 522. Detection module 210 may receive any encrypted response from lock tag 112 and compare at block 524 the response received from lock tag 112 to the response received from key tag 1114. Thus, for each response

received from a lock tag 112 in a given round, detection module 210 may compare a response from a key tag 114 received in a previous round to determine if the log tag 112 and the key tag 114 contain matching encryption keys. In the event a match is not found within a predetermined period, for example within a few rounds to allow for data loss, detection module 210 may generate an alarm at block 526. In the event a match is found within the predetermined period, then an alarm is not sound, and in addition a successful match may be indicated, although the scope of the invention is not limited in this respect.

[0027] In the embodiment of the invention as discussed with respect to FIG. 5, the encrypted nonce in responses received from key tags 114 and lock tags 112 may be compared to verify that lock tags 112 possess matching key tags in the vicinity. Since a key tag 114 provides a response containing the encrypted nonce in the round prior to the response broadcast by a lock tag 112, generation of a new nonce may invalidate subsequent responses from key tags 114 so that a spoofer or an attacker may be prevented from providing a false matching response after a lock tag 112 provides its response. In such an arrangement, a false or a spoofed key tag 114 may be prevented from merely duplicating a response of a lock tag 112. In one embodiment of the invention, in the event an invalid or a spoofed lock tag 114 generates an encrypted nonce stream with no matching key, an alarm may be generated, and it may be difficult to create an invalid or a spoofed key tag 114 that matches an existing lock tag, although the scope of the invention is not limited in this respect.

[0028] Although the invention has been described with a certain degree of particularity, it should be recognized that elements thereof may be altered by persons skilled in the art without departing from the spirit and scope of the invention. It is believed that the radio frequency identification tag lock and key of the present invention and many of its attendant advantages will be understood by the forgoing description, and it will be apparent that various changes may be made in the form, construction and arrangement of the components thereof without departing from the scope and spirit of the invention or without sacrificing all of its material advantages, the form herein before described being merely an explanatory embodiment thereof, and further

without providing substantial change thereto. It is the intention of the claims to encompass and include such changes.